



Jeffrey M Moritz <jmoritz@eiproject.org> on 01/30/2002 04:17:22 PM

Please respond to Jeffrey M Moritz <jmoritz@eiproject.org>

To: vss@FEC

cc:

Subject: Comments submission

Dear Ms Bonsall

Please find attached our email submission regarding comments to the Proposed Standards dated December 13, 2001.

The Election Integration Project, Inc.
Jeffrey M. Moritz
Warren J. Rutherford



- att1.htm



- fec_response-final.doc

A Not-For-Profit Company
426 North Street, Hyannis, MA 02601
Tel: 508.771.6500
Fax: 508.771.1119

January  30, 2001

Ms. Penelope Bonsall, Director
Office of Election Administration
999 E. Street N.W.
Washington, DC 20463

RE: Submission of commentary on proposed Voting System Standards


Dear Ms. Bonsall,

Please find attached our comments regarding the issuance of revisions to the Voting Systems Standards posted on December 13, 2001. We have submitted them to you electronically along with a copy forwarded to you via land mail.

We thank the Commission for the opportunity to respond.

If you keep a mailing list, please include us thereon.

Very truly yours,



Warren J. Rutherford

Jeffrey M. Moritz
Chairman
jmoritz@eiproject.org

Warren J. Rutherford
C.E.O.
wrutherford@eiproject.org

TABLE OF CONTENTS

<u>THE ELECTION INTEGRATION PROJECT</u>	2
<u>Mission</u>	2
<u>Activities</u>	2
<u>EIP's Leadership</u>	2
<u>Relevant Technological Experience of Current Technical Members</u>	3
<u>ISSUES THAT FACE THIS ENDEAVOR</u>	4
<u>Standards Design and FEC Goals</u>	4
<u>New Standards Not Exclusionary</u>	5
<u>Cost of Development and Testing</u>	5
<u>Trustworthiness</u>	6
<u>Procurement Standards</u>	7
<u>SYSTEM STANDARDS DEVELOPMENT</u>	7
<u>The December 13 Draft Document</u>	8
<u>Confusion of Terms</u>	9
<u>MISSING FROM THE STANDARDS</u>	9
<u>Common Criteria Testing</u>	9
<u>Registration System Integration</u>	10
<u>Standards for Internet Voting</u>	11
<u>Using Open Standards</u>	11
<u>COMMENTS ON PROPOSED STANDARDS</u>	12
<u>Security and COTS</u>	12
<u>Access Security</u>	13
<u>System Security</u>	13
<u>Software Accuracy, Recovery and Testing</u>	14
<u>Limitations on Software and Module Size</u>	16
<u>Redirection Prohibition</u>	16
<u>Acceptable Error Standards</u>	16
<u>Telecommunications</u>	17
<u>Accessibility for the Disabled</u>	18
<u>Electrical Provisions</u>	18
<u>CONCLUSION</u>	19
<u>Accepting Change</u>	19

THE ELECTION INTEGRATION PROJECT

Mission

The Election Integration Project Inc. (EIP) is a Massachusetts Not-for-Profit Corporation organized to promote the development and dissemination of election reform standards, procedures, and systems that will ensure effective voter registration and the orderly and accurate conduct and count of elections through out the United States. An additional mission of EIP is to provide educational and informational resources for persons, municipalities and organizations concerned with these voter registration and election procedures.

EIP commits to these activities to help ensure that public confidence in this most basic sovereign right will be restored through systems and procedures that utilize a set of "*best practices*". Without the commitment from independently and publicly funded organizations (such as EIP), which objectively advance voter registration and election system reforms, the accuracy of the outcome from the exercise of that sovereign right will continue to be in question.

Activities

EIP's activities are divided into three primary categories: (a) standards research; (b) educational and informational resource development, and (c) professional assistance to governmental entities. For purposes of this submission, this document will focus solely on the standards research.

As part of fulfilling its first mission, EIP's research of standards has included information about alternative approaches to systems, comparisons of existing systems, and systems management. That search also has pursued discussions with engineering and security professionals about industrial and governmental solutions to problems similar to those that exist in the current election process. EIP believes that this process will identify and develop an overall set of appropriate and all encompassing "*best practice*" standards for use in election management systems. These standards will be submitted to the Federal and State Election Commissions for their consideration and future inclusion.

EIP's Leadership

EIP's Chairman and CoFounder is the Senior Partner of a management consulting firm which has, for over 20 years, consulted to both domestic and international companies in systems integration, defense systems contracting, high assurance internet security systems, software development, mission critical computer based training, manufacturing, financial products and Internet services. His services included: management and operational analysis and reorganization to improve operations performance, design and implementation of internal control systems, and strategic planning.

EIP's C.E.O. and CoFounder has worked in leadership roles for municipal government for over 23 years including town manager and fiscal officer. He has taught graduate courses in Public Administration, Financial Administration and Organizational Behavior. He currently serves as a consultant to several communities using his expertise in organizational management, human resource management, organizational restructuring, strategic planning, cost bench marking, financial management, revenue and program forecasting, productivity improvement, program analysis, continuous quality improvement, and performance measurement systems.

Relevant Technological Experience of Current Technical Members

The founders are supported by a team of staff and consultants who possess their own leadership skills, technical knowledge, management expertise, and commitment to excellence in governance necessary to accomplish EIP's objectives.

EIP's Consulting Security Architect is currently the senior engineer and security architect responsible for security services integration on a high assurance kernel platform. He was responsible for the design of the Novell Enterprise Authentication Service to integrate Single Sign-on, the Multi-Authentication Framework, and multi-system background authentication. He is the holder of more than eight U. S. patents

EIP's System Integration Consultant has over 30 years of experience in technical consulting, research, and executive management for high technology organizations, academic institutions, and government agencies. He was the founder of two high technology engineering firms specializing in creating unique computer-based information systems for various U.S. Government and Department of Defense agencies as-well-as large commercial enterprises. He has been an invited speaker and panel moderator for several symposia concerned with computer assisted training and education.

EIP's Consulting Distributed System Engineer developed the network security and disaster recovery architecture for a Fortune 100 international corporate system, designed and installed a large multilevel secure fiber optic system for a U.S. Government agency, and designed and implemented a large (1,400 node) fiber-optic network for a state university.

Each member of the team has a reputation as a creative thinker and competent achiever in their respective disciplines and has contributed to the furtherance of technology or excellence in governance in today's society. They lend their expertise to EIP by focusing their combined efforts on the development of better and open voting system standards.

ISSUES THAT FACE THIS ENDEAVOR

In order to achieve the most appropriate solution to election management reform, it is necessary to acknowledge the converging events that brought this need into sharper focus. Although there is no question that the general public no longer trusts the existing system to provide an accurate count of the votes cast in any election, new voting system procurement has been a low fiscal priority. There was debate regarding the need for more advanced systems but there was, as yet, no understanding of the advances in technology that could be used. There were escalating costs of system design, testing, marketing and maintenance that deterred the funding of replacements for antiquated systems. The events of the 2000 Presidential election merely moved the need for improvements up on the priority list.

Standards Design and FEC Goals

There are two perspectives on the method for development of election standards – (1) should the standards describe what the mechanism is called upon to do (*what's*); or (2) should it detail how this mechanism is going to function (*how's*). Based on the election system standards promulgated by the FEC in the posting, the lines between the *what's* and *how's* are blurred. We believe this may exist in an effort to safeguard the trust of the public, promote competition in development, and provide a guideline for state and municipal procurement. The lines are further blurred by the inclusion of some *functional standards* that are really a combination of both *how* and *what*, but avoid requiring vendors to answer questions regarding how their systems meet the standards. We have always believed that EIP's overall mission is in concert with the FEC's mission, as we understand it. We strongly believe that there are alternative approaches and additional benchmarks that promise a much more encompassing result. The lack of distinction between the *whats* and *hows*, and the inclusion of more trustworthy *functional standards* could be useful mandates to encourage the development of better systems if portrayed in that light.

We also perceive that the efforts by the FEC to establish these standards are based on two additional perspectives: (1) a vendor sensitive playing field; and (2) elementary practices in system design standards that make the vendor systems easy to test and review. These may intend to level the competitive field for different types of technologies and, perhaps, even support independent testing, but we do not believe that this method fosters "best practice" development. We believe it inadvertently sanctions lowest common functionality.

Some of the FEC's goals, unfortunately, have not been met. Economics has become a more significant factor. The rising costs of system design, manufacturing, testing, and marketing for these systems; a demand for more functionality; and a limited market size; have all created a lower than anticipated quality or functionality in the system designs. By trying to overcome cost, the FEC's design criteria has forced the combination of backward-compatible standards for multiple technologies that do not share similar capabilities. The design criteria, of necessity then, also includes the use of antiquated approaches and techniques that are influenced by older processes, even though their failures are known. This promotes distrust.

New Standards Not Exclusionary

The Congress has recognized the need for improved election system standards by funding research and procurement. The FEC (and NASED) must consider the long-term significance of their current efforts and avoid the tendency to rush the development of new standards until all options can be considered.

As a solution to the short-term pressure from Congress to "fix it" while the longer-term issues are resolved, we believe the Commission has the opportunity to draw a line now, establishing standards that no longer permit the use of unreliable systems and processes, and as a result, mandate the development of new systems and processes for the future through more advanced standards. If the existing systems cannot comply, they become uncertified and therefore unusable. This will necessitate the procurement of updated systems and the development of retrofits by the vendors of the technically capable ones.

Cost of Development and Testing

When it comes to procurement and standards, the existing recommendations by the FEC defer to State's rights. This creates the potential for technical certification up to 51 times, measured against 51 different standards, for the same product. This is costly to the vendor and is a bar to the entry of new companies interested in pursuing this market. Effectively, instead of being a competition driver, it is anti-competitive to smaller companies who may have products that are technically superior.

Consider the paradox that most of the research today is done by corporations that already have a major stake in their industry. Because of their position, it is counter-productive for them to change the status quo. It is an easy, but inappropriate, theory to think that new or advanced methods and specific procedures of configuration management should be left totally to the vendor's decision. It is equally easy, but inappropriate, to assume that those procedures would result in a configuration management operation that would meet a high enough standard. Any really new idea might detract from market position and profitability, so those companies best qualified to do the research to develop new approaches are the ones least likely to take advantage of it. It is this paradox that fosters the development of break-through technology by small companies meeting the challenge. It is up to the governing agencies that require this research to proactively set the bar as high as possible without making the gates to entry exorbitant.

The strengthening of NIST and/or ITA as acceptance testing centers for all jurisdictions is a key ingredient to resolving the problem of expensive system pre-deployment costs and elementary programming practices which are necessary for system review. EIP supports four initiatives that support this concept: (1) the notion of a single Federal set of standards; (2) funding for the NIST/ITA for up-to-date equipment and highly trained personnel needed to accomplish their expanded mission; (3) standards that are high enough so that the States will

gladly accept them, and NIST/ITA can test them effectively and efficiently; and (4) the use of open system and open standards development to reduce the cost of entry to smaller companies.

Trustworthiness

Questions about the need for integrated electronic voting systems in the United States have been based upon common misconceptions. These perceptions embraced the idea that vote fraud today was not a big problem and therefore new systems were not needed. They encouraged the idea that today's elections were more honest because of changes made over the past 150 years to the **processes** used to conduct elections. In truth, these changes have not made voter or voting fraud impossible, just slightly difficult.

Example: Missouri's Secretary of State announced that, among 1,384 ballots known to be illegally cast, there were at least 62 by felons, 79 by people registered at vacant lots, 68 by people who voted twice, and 14 cast in the name of dead people.

Example: Voters continue to be required to use inherently flawed punched-card systems or other voting approaches which are no better. Optical or magnetic sensitive (mark-sense) systems suffer from many of the same problems described above. Lever-style voting machines offer more security, audibility, and a significantly better user interface, but these devices have other drawbacks -- including the fact that no new ones have been manufactured for decades. Paper ballots become less and less practical as a voting mechanism as the need for more functionality increases.

There are current recommendations to rely on the existing products and infrastructure. A brief review of what is available indicates that most of the current offerings are a "technology enhancement" to an existing method, rather than a true new solution. In considering the Internet, the current consensus rightfully indicates a realistic distrust of the accuracy, trustworthiness and security of any Internet based vote management system - even those using smart-cards, PINs or similar ideas. The country cannot really begin to seriously explore the full generality of Internet voting from personal computers until it has a base of experience with trustworthy networked voting systems that are fully under the control of the municipality, county, and/or state. Even the concept of having software platforms that are separate and distinct from existing computer operating systems and web browsers will not guarantee any level of trust by the voting public. So the true FEC mission for standards must address not "Who can you trust to run a fair election?" but rather, "How can the FEC define a trustworthy electoral system when none of the participant systems are trustworthy?"

Those who conduct elections have encouraged their respective populations to believe in the honesty of their elections. November 2000 and September 11th changed all that. It focused on the simple premise: Freedom matters and the protection of freedom is through the vote. Society now demands a better system to manage that "protection" as it is too important to be left to inferior apparatus. It is not unreasonable to concede that any system developed should look at different avenues for registration, authentication, balloting, tabulating, and process

security through the review and re-engineering of the entire process.

Procurement Standards

In providing guidance to governmental officials, the higher standards proposed by this commentary could form the basis for a set of comprehensive procurement guidelines. This would mitigate risk for those officials by not requiring them to become experts in voting system technology. This also would place a greater burden on vendors to demonstrate compliance with the NIST/ITA and FEC-VSS standards. Consider the following example:

Example: In the Commonwealth of Massachusetts, there are 352 political jurisdictions that are responsible for the procurement of election management systems. Each jurisdiction must now obtain these systems through a competitive procurement process. Currently, each procurement process must locally develop review guidelines. Due to the absence of common standards, these process guidelines can only be established by soliciting sample system specifications from the vendors. This solicitation creates the risk for the jurisdiction of engaging in "sole-source", and not competitive, procurement.

Does the FEC, in not desiring to impinge upon local decision making, want to allow a continuation of inconsistent election systems procurement practices or does it wish to provide objective and technical guidance to those responsible jurisdictions? The FEC is in the unique position to provide procurement and election officials a higher level of confidence. The election systems purchased will be more reliable in their operations than present offerings on the market and conform with a competitive procurement environment. This role would help ensure the implementation of more trustworthy election systems.

SYSTEM STANDARDS DEVELOPMENT

After the last federal election cycle, there are few people that would argue that a better system is needed to insure that all the votes get counted – and counted properly. Society is demanding a change. Nothing made that more clear than the post 2000 Presidential elections outcry and the subsequent political discussion. However, in their rush to prevent "another Florida" in their own jurisdictions, many legislators and election officials mistakenly believe that simply more computerization is the solution. That could not be further from the truth. The best solutions will come from the solidification of standards that encompass not only registration management but the election process as well. But systems adopted from common, day-to-day applications, will not be viable as voters will not tolerate unreliability or insecurity. These standards must also promote competition and compliance by which objective comparisons can be made.

In that context, then, the primary goal of the Voting System Standard is to provide a vehicle for state and local election officials so that they are able to assure the public of the integrity of election systems – mechanical, paper or computer based. The methods for achieving this goal, however, have broadened with the advent of a demand for more sophisticated and integrated

systems. The draft of the VSS being offered provides a common set of requirements across all voting technologies. It uses technology-specific requirements only where essential to address the impacts on voting accuracy, integrity, and reliability unique to a particular technology. We believe that approach may be flawed.

The challenge in establishing new standards is to make sure that any new processes and/or technologies enhance the availability and experience of voting and close possibilities for fraud without introducing any new ones. This cannot be done with the same set of minimum standards applied across paper, manual, mechanical and electronic systems for no other reason, than the difference in their functional capabilities. That sets the bar too low and encourages the lowest acceptable functions at the highest cost. So long as standards for systems and processes enlist this lowest common standard, there is less likelihood that sophisticated, safe, and secure systems will be offered. There is no economic mandate otherwise. Providers will neither advance the election systems ability to have security verified by external agencies, nor provide a method for limiting voter fraud, nor extend the reliability of the systems without such an inducement.

The December 13 Draft Document

As an overall view to the content of the document, it appears that it is attempting to fulfill three missions at once: (1) describe the technical standards; (2) describe the voting process standards; and (3) describe a set of procurement guidelines. However, in doing so in a single document, the reader is easily confused as to the technical nature and importance of each paragraph as it alternates between the three. In the effort to curb that confusion through the use of non-technical terms, the document waters down the importance of a standard, or worse, makes it totally useless in fulfilling its intended purpose. As a result, it might be beneficial to separate the document into three separate publications. In this way the need to provide in-depth descriptions can be done so with the use of terminology specific to each requirement and with standards that are written for those who are actually called upon to produce the component.

Example: In a targeted technical offering, the disparities between paper, mechanical and electronic requirements can be managed by describing the specific standards for each different type of component, separately using language that would have engineering significance. This "completely drawn" set of standards could provide for a higher level of technical competence without tending to confuse the measurement of those standards and ultimately price the voting systems out of the range of local jurisdictions. These standards could actually reduce the cost of production, as they would open the door to competitive practices within any given device built to a standard and lower the testing difficulties and costs.

The same may be said about software standards. Common code sharing (open source) and the avoidance of confusion in interfacing code (open standards) are but two examples. Strong software standards contribute positively to the reliability and maintainability of software – particularly on larger projects. If well constructed, such standards also have a major impact on

reducing life cycle costs. Although reliability and affordability are obviously important attributes for an election management system, it is impossible to ignore the need for accountability (proof that the system performs according to the approved functional specification) and system security (necessary to ensure that the "one man one vote" concept is fulfilled). Both accountability and security are heightened by the use of "Open Standards" and "Open Source" as they open the logical operations of the software to the necessary scrutiny. The same cannot be said for proprietary commercial off-the-shelf systems.

Confusion of Terms

The proposal draft's use of "public domain", COTS and "proprietary software"(sometimes interchangeably) when compared to the industry accepted definitions, creates a confusion in concepts and could deny the less technically oriented the ability to make intelligent decisions based on the application of this publication. We offer the following narrative regarding COTS software for consideration:

COTS software can be either (a) "open source" defined as that software whose internal designs and codes are publicly published and otherwise made available on an unrestrictive basis; or (b) "proprietary" being defined as that software whose internal designs and codes are **not** published for public consumption or otherwise made available on an unrestrictive basis and which has more restrictive licensing or purchasing requirements. Non-COTS (sometimes referred to as "custom") software is that software explicitly created for a single entity or purpose that is not made generally available in the commercial market. It is either used only by the original creator or the organization that had the software created or by the original creator and a small list of other organizations to which the software is made available.

The opposite of "proprietary" software, therefore, is not COTS but rather "open source" software.

Example: Microsoft Windows Operating Systems (95/98/Me/2000/XP/NT) are all proprietary and the UNIX or Linux Operating Systems are open source. Both are COTS.

It would help to clarify this potential confusion by using the term "Non-COTS" as the opposite of "COTS". It would be defined as a type of software not generally available to the public and carefully restricted in its distribution. Consider using "proprietary" and "open source" to differentiate between software whose operational characteristics can only be determined by exhaustive testing (proprietary) or by testing and visual or AI-based scanning (open source).

With respect to voting systems, it is clear that operating systems software, database management software, word processing software, etc. are largely COTS. Note that COTS is almost always proprietary.

MISSING FROM THE STANDARDS

Common Criteria Testing

The computer industry had established standards for secure system certification, and such certification was typically performed for devices purchased by various US Departments and Agencies, including the Defense Department. This had been mandated by Congress under the Computer Security Act of 1987 (CSA87). Congress, however, exempted itself from compliance with the Act. As a result, they have never certified the accuracy and integrity of any computer-based voting systems used in any Federal elections under those standards. Recently, newer standards for security certification were established in conformity with a worldwide agreement.

A well-known computer scientist and respected voting system expert, Rebecca Mercuri recently stated:

" if a computer voting system vendor wishes to claim that their system is secure and accurate, they should voluntarily submit their product for certification under the new Department of Defense standard, known as the Common Criteria. The Common Criteria has 7 levels, and level 4 would be the minimum level appropriate for use with voting systems. NIST should be authorized to conduct such evaluations, and in the meanwhile, national standards for voting system assessment can be formulated, and appropriate laws passed. Recently, a major software manufacturer, convicted of unfair business practices, announced its intention to form a consortium for the creation of new voting systems. Only a few months ago, this same firm admitted to having been the recipient of a lengthy undetected Internet attack on its own proprietary [and allegedly secure] materials. Should a monopolistic organization, incapable of protecting its own assets from malicious hackers, be entrusted with our country's votes?"

In essence, what the expert alleges is that the computer industry's currently offered voting systems are *"nicely packaged Pandora's boxes of unverified software and insecure hardware."* If municipalities continue to procure these boxes, whose contents they do not know or understand, on the basis of "trust us" recommendations from the manufacturers, one thing is certain. *"Some years down the road the box will open to reveal yet another election fiasco, but this time instead of hanging chad, we will have disappearing electrons. Next time, there will be no recount since we will be told, like some voters were in New Jersey, that "no votes were ever cast."*

Registration System Integration

The comments associated with "integration with the voter registration database" state that *"the design and interface between the voting system and the voter registration database has been explicitly excluded.... for practical reasons."* The document states that such a standard will be promulgated *"at such time when the majority of voting systems and voter registration databases become more seamlessly integrated"*. This is inconsistent with the need to establish standards proactively rather than reactively. The time to specify principles is now - to ensure that the standards governing the design, performance, functionality, and testing are

appropriate. At the very least, standards are needed to address the interface between voter registration information and vote tabulation systems to ensure the sanctity of the vote.

Example: In a statement from Senator Kit Bond (MO.) he said that [amazingly] 247,135 of St. Louis' 258,532 voting-age residents were registered to vote. That incredible 96% registration rate was obtained in part, he said, because almost 1 in 10 voters registered in St. Louis was registered to vote somewhere else as well – that is about 25,000 double votes just in one city.

Example: Another disclosure indicated that of 1,268 Missouri applications for court orders which were intended to secure the vote (for voters who were allegedly removed from the voting rolls by mistake,) 1,233 were improperly granted, many for people who admitted they had never registered.

Should the Commission fail to include the specifications for integrating voter registration with voting tabulation now, by the time registration integration has occurred, it will be too late and too costly to fix. At that time, the only possibility for the FEC would be to retroactively decree every standard appropriate based on whatever integration technology the vendors had provided. Should those integration standards be unacceptable, the consequence would be the necessity of funding the cost of replacement.

These integration standards would also provide more opportunities to enhance voter participation. The use of alternative locations for voting would offer the possibility of voter participation for any given jurisdiction, up to and including statewide elections, without regard to the physical location of the voter or the voter's precinct. This would certainly increase voter participation by supplying more convenient means to participate.

Standards for Internet Voting

EIP agrees with the notion that Internet voting is not practical at this time. It should be noted that California, Arizona, New Jersey, New York, Texas and Florida, to name a few, have all initiated commissions to study the possibilities of new technology voting on a wider scale. However, we believe no expert would tolerate an Internet dependant voter system subject to the level of abuse that is present in the world of e-commerce. Furthermore, the use of Internet connected computers in the voting process raises serious security concerns that have no parallels in the world of e-commerce and, as yet, have no practical solutions.

This decision, in and of itself, is the very framework from which an appropriate set of standards can be built. If something does not meet standards (at least not yet), then the reasons they are not met, are known. Therefore, those reasons are the equivalent of a standards requirement. If Internet voting is ever to be, the time to establish the reasonable standards is now.

Using Open Standards

It is clear that the larger the number of people that use a specification the more likely the specification/product will be considered a standard. Such standards are known as *de facto standards*. They have become standards not by intent of their creators but by acceptance (reactive). On the other hand, some specifications become standards from the moment of their inception. These standards, known as *open standards*, are developed by a group, committee, or consortium of interested or directing parties or by a government agency in advance of development (proactive).

Today, two 'standard' operating systems have emerged: (1) the proprietary Microsoft Windows standard, a *de facto* standard because of its hold on the desktop computer market; and (2) the *open system* POSIX standard, with which all versions of UNIX and LINUX are compliant. Most of the Internet infrastructure and large government and corporations networks are based on this same POSIX standard. IBM is spending \$2 billion in translating their software to LINUX, an *open standard*. Although initially more difficult for the layman to use than the *de facto* standard, it is chosen because of its stability under high levels of utilization, its relative efficiency in the use of resources, and its reliability and security, proven by years of development and use.

The voting industry has been characterized by a lack of common standards, which would enable even the simplest transfer from one operating system to another. Each manufacturer has its own system and each has its own prescriptions for how programs are integrated into the system. This lack of compatibility "locks out" a competitive vendor from a municipality's installed system. EIP does not believe this is what the VSS intended, but the ambiguous standards have created a multitude of distinct subsets none of which are easily compared functionally and none of which can be used together. This hinders development and procurement.

EIP believes that the concept and use of open source and open systems should be mandated for any public system application requiring strong security, regulatory oversight, and competitive encouragement. Such code can be readily scrutinized, edited, and built to meet specific requirements prior to application development. Once built, any developer of those applications, by using this open source and an open standard, is capable of building programs that comply with the security requirements without the fear of breaching regulatory oversight. What is produced from that competition, eventually, is a "best of breed". And further, if all vendors employ open systems standards, the range of experience required by testing labs will be decreased, thereby making it easier and less expensive for them to perform the highest quality work.

COMMENTS ON PROPOSED STANDARDS

Security and COTS

The VSS draft states "*devices and software [COTS hardware and software] are exempt from certain portions of the qualification testing process so long as such products are not modified*

in any manner for use in a voting system." If security is to be considered a critical concern than this perspective is ripe with pitfalls.

The Commission must not consider accepting any software without at least security testing. Many technology professionals believe poor quality and insecure software remain the largest problems for users of commercial offerings (COTS). Even Carnegie Mellon University's CERT Coordination Center says the number of software vulnerabilities reported on COTS software last year was more than double. The National Infrastructure Protection Center's 2001 summary of software vulnerabilities, now over 70 pages long, includes software from all types of applications -- and all are commercial-off-the-shelf.

What needs to change is the software engineering culture. Fault prevention should happen during the design and development process rather than hoping to catch faults during testing. Without appropriate development and testing (whether conducted directly by the ITA or reviewed from other organizations' test results by the ITA), any system based on COTS technology has a propensity for operational and security failures. The larger and more complex the software, the more propensities exist for faults. **Ignoring this by exempting COTS from testing, especially security testing, is a formula for tragedy.** The FEC/NASED should consider incorporating the Federal CSA87 mandate and its security standards in Common Criteria. They should seek the help of other agencies with experience in this area or face the possibility of finding that the systems that meet their standards are suddenly at substantial risk. Other federal agencies, such as DEA, FBI, CIA, DIA, and the INA, who had similar exemptions, were embarrassed by their lack of security before sharing their knowledge and solutions post 9/11.

Access Security

What professionals in computer security know is that the people who follow the rules and regulations are not the problem. Perhaps it might be useful to indicate the level of technical sophistication of the threats against which systems must be defended. Is security needed just to protect from inadvertent manipulation by election officials running the application, or must attacks from highly sophisticated hackers also be included? A generalized statement regarding the need for security access controls is important but, as a standard, it is probably insufficient. The pertinent paragraphs of the VSS might be rewritten to provide for access protection systems that would be developed according to a stipulated set of standards that would be difficult (or impossible) for most casual users to defeat.

Example: The following questions should be resolved: (1) what is the definition of a "critical system component; (2) what is detection of access in real time required; (3) should the "critical component" be smart enough to determine the permissibility of an access, or (4) is access being managed by an untested COTS operating system environment?

The objective of access control security is not to deny somebody fixing something, the ability to override a control or application that has demonstrated a fault. This requirement can best

be left to physical security people with access restrictions (i.e., by requiring pairs of people to do such work), in conjunction, perhaps, with special and controlled sets of access keys whose physical security would be the most important element of all.

System Security

The industry recognizes that in recent computer attacks, it wasn't the communications paths that were compromised, but the security of the servers themselves. In heeding that warning, EIP supports a well-structured and coherent set of questions that have been proposed for use by Rebecca Mercuri (a well known voting system expert) in conjunction with the security evaluation of any electronic balloting and/or tabulation system under assessment. EIP included these for the Commission's review and suggests that an appropriate restatement of these questions would form the basis for standards which could be included in the revised version of the VSS. The questions are grouped by category for purposes of this presentation and not necessarily in their order of importance.

Voter Authentication and Vote Security

1. How are voters authenticated and authorized to cast ballots?
2. What access controls are in place to ensure single ballot per voter per election?
3. If multiple systems are deployed, how are voters tracked so the same person does not vote in different formats?
4. What means are used to separate voter identity from voted ballot?
5. How is the auditing process precluded from associating the voters with their cast ballots?
6. How is the balloting process secured so that no voter submissions can be observed, or recorded in any way that is traceable to the individual voter?

Tabulation Security

7. What controls are used to ensure that the correct ballot is provided to the voter?
8. What actions on the system are audited?
9. How is the audit trail accessed and used?
10. Who is permitted to access the system (through all aspects of handling)?
11. What controls are provided to ensure that each ballot item is voted properly?
12. How does the system assure that each ballot has been correctly recorded?
13. How are all forms of tampering detected and prevented?
14. How is vote confirmation provided without ballot-face receipt?
15. How does the voter know that a cast ballot has been accepted?
16. How is vote tabulation correctness assured?
17. What facilities are provided for recount purposes?

System Functionality

18. What features are employed to ensure operability of the voting system throughout the election?
19. How are downtimes handled in the event that they do occur?
20. How do the poll workers and system administrators know that the system is operating correctly?

21. How is the voting system precluded from use when deemed inoperable?

Software Accuracy, Recovery and Testing

No one can "ensure" that proprietary software meets high security standards without appropriate and exhaustive testing, so there is a need for some caution. As an example, the security holes in Microsoft operating systems existed even after the millions of person hours (and dollars) were spent in testing. They spent millions more afterwards to rectify security breaches found by teenagers. In applying the proposed standards of system "accuracy", the standards must provide a measurement for testing accuracy, especially when the program runs in an insecure, low integrity, and unreliable operating system which is otherwise exempt from testing.

A perfect application program's intent can be foiled through an external influence by accessing the data while the data is recorded. Even one that professes logical correctness may not be accurate. A program can be completely, logically correct, but still be unable to perform the intended function.

If we accept that the operating system elements of any automated system are essentially built by an "external" provider, and that the operating system is provided to the system vendor as COTS to be incorporated into the voting system (without changes that might be required), it passes by all standards without testing, regardless of its functionality or lack or security. However, if the vendor adds security provisions or improvements, then by definition, the operating system has been modified and it has to meet standards and testing requirements. That is counterproductive to a "best of breed" or "best practices" perspective, and, at the very least, contrary to the precepts of security, reliability, and validity on which this document is focused.

The proposed standards appear to differentiate between catastrophic failures from internal and external influences. We believe this to be in error. It might be better to define "catastrophic failure" as one which cannot be either (1) automatically rectified by internal hardware or software mechanisms; or (2) repaired by human intervention within a specific period of time (such as a few minutes). As such, all software used in a voting system, (COTS, proprietary or custom) could be rigorously tested against an acceptable standard of recovery so as to provide another safeguard from voting interruptions or irregularities.

A caution is necessary with regard to "public domain code" being categorized along with COTS for this testing exemption. There is no reason why public domain code, if used, shouldn't be commented and structured just as rigorously as new code. After all, any such "public domain" code should be checked for validity, applicability, or logic problems as well. If it is not checked you have a wide-open security hole.

Consider, then, the development of a specification requiring the use of an open source operating system (as previously defined). In general, such systems are more responsive, more available, less quirky, more reliable, much more secure, and less expensive (cost of

developing and maintaining software is less, for example, as is the initial license cost of the software [which may be virtually zero]). There is also a much better understood mechanism for stripping operating system software of all unnecessary applications. Any maintenance and support software can be run on the target system from a separate maintenance system, which could have its own unique level of security.

Limitations on Software and Module Size

As a company with principals that have years of software experience, EIP understands that software often calls for sub-routines or modules for specific repetitive tasks in its coding. They are, however, neither a design criteria in and of themselves, nor are they normally limited in length artificially. Sixty lines of code represent approximately one page, which cannot accomplish much, if you are using C or C++ and including headers and comments as well.

Using smaller and well-named modules as a standard of software design is not necessarily inferior, but there will be so many of them that: (1) they will have to be managed by some kind of development support program (would this be considered a module?); and (2) the system will spend almost as much of its time moving between modules as it will doing useful work. Following this logic, having one main in and main out "flow" is normal, although it is reasonable to also have error exit flows. These error exit flows seem to be prohibited, however. Traditionally, there are many locations where control leaves the module, and returns, - e.g., at every subroutine call, macro call, etc. To add to the issue, as the standard seems to require non-I/O errors to be handled within the routine, it forces the routine to be too short to accomplish its designated mission and error management. This specification is overly restrictive albeit easier for testing. Experience tells us that artificial restrictions in design are paid for in performance and development costs.

Redirection Prohibition

EIP's interpretation of the provisions of Section 4.2.4 (b) concludes that it does not permit redirection of control by means of operator intervention or data-driven logic. Although we understand the rationale, two questions arise. (1) Without such intervention, how is a problem program stopped in order to correct it? (2) Why is there a prohibition of data driven logic? The simplest example of data driven logic is associated with response to a clock, response to the condition of a buffer, the monitoring of system status or data quality, or in this case, response to the number of votes tallied, or whether or not the vote contains a write-in, etc. It appears that the intent is to permit the systems used for software testing, to track subroutine calls. This does not guarantee that these testing systems will discover everything the subroutine may do. Or is it that the testing systems cannot track logic branches based on data? In either case, there appears to be a need for clarification.

Acceptable Error Standards

A realistic target rate for ballot error should be advanced in light of the nature of how

elections are tabulated and segregated by what or who potentially commits the error. There should be different target rates for equipment (hardware and software systems) and for humans operating the equipment. Attempting to establish the same standards to equipment and human error rate in the operation of the equipment would certainly cause large debate, and any such definition would likely have fatal flaws.

For equipment, a realistic testing error rate for tabulation hardware systems could be in the range of 1 in 10M... a value that is easily obtained with any modern computer system that invokes internal error correction. In reality, some hardware has a higher data error rate than realized, but those rates are dropped to near zero after the application of error correcting procedures in the system firmware.

As for human error rates, selection feedback mechanisms design should anticipate that a voter would have to make the same error twice – once when recording a selection and again when verifying that the selection was intended. If the concept of such ballots-cast-in-error were allowed, procedures that attempt to infer what a voter intended to do would be required. They would be totally subjective and could not determine what the voter actually did. They would be subject to the same suggested error rate standard applied to the equipment. Just as “security cannot be absolute”, so neither can a lack of voter error be avoided. Instead, mandate a creditable mechanism for feedback. Thereafter establish that it is the voter’s responsibility to ensure the vote is cast as intended.

We support a concept of “human error rates” that is limited to any manual procedures other than the actual process of casting the vote on electronic systems. As an example, and notwithstanding the objections of some civil rights lobbyists, there is a new Florida law that requires signs at polling places reminding voters of their “responsibilities”. These include: keeping their address current; bringing proper ID to the polling place; knowing how to properly operate the voting equipment; asking questions when they are confused; and checking the completed ballot for accuracy.

Telecommunications

In defining telecommunications under Section 5, the VSS draft chooses to ignore the differences between locally connected and remotely connected systems. Nonetheless, it still goes on to establish that the components shall meet the same accuracy, durability, reliability, maintainability, availability, integrity, etc, standards even though the specifications should be different.

Section 5.1.1 covers standard ‘networking’ technology, but ignores other potential interconnect technologies such as IEEE1394 and USB – both of which are important in connecting “dumb” passive reporting devices such as printers and displays. Section 5.2 does not differentiate between short-haul transmissions, such as cables installed in the same room when the polling place is set up, and long-haul transmissions, whether over private or public networks. Section 5.3, establishes prohibitions against a list of seven specific items based on assumptions as to the state-of-the-art of network security. (We recognize that this expertise

may not have been available to the Commission based on its membership list and available testimony.) However, based on the draft's definition of telecommunications, we believe that vote data could not even be shared among machines in a cluster. As a result, concepts like centralized shadow (redundant) recording to backup systems on a network would be unavailable as a means of securing voting data.

We believe it is important to make the intent of this standard clear. We understand that when voting information is passed from any system device to any other system device (other than printers, displays, and other similarly passive reporting components) the transmission should include a handshake (confirmation and acknowledgement) which advises the sending system as to the success or failure of the transmission. Perhaps a rewrite of the definition of telecommunications is warranted. The sole intent would be to define it as the vehicle for the communication of voting information between subsystems that create it and those that further store and/or process it. Under such a definition, there would be no need for concern about printer and display connections, as they are not tasked with communicating fragile and/or irreplaceable information between subsystems. Also, there would be no worry about whether the vendor needs to be limited in the use of those technologies in Section 5.1.1. For example, IEEE1394 or USB are perfectly reasonable technologies, assuming they meet the standards of Section 5.2.7 when used to pass voter information.

Accessibility for the Disabled

The Voting System Standards approach the physical access requirements for the handicapped by stipulating that the access requirements apply to all systems, and significantly more requirements apply for DRE systems. Consider the possibility of a different set of standards - that of two separate and distinct systems which both must be available at any polling center. The primary difference between the two would be the approach to the physical requirements of accessing the ballot, affecting the vote, and receiving feedback.

The first set of standards would meet the needs of the majority of people without disabilities and would be applicable to all systems regardless of technology. From a practical perspective, the cost of manufacture and the ongoing maintenance for the non-disabled systems would be reduced substantially and the overall savings in procurement costs would be reflected accordingly. In some ways this could be considered a "stripped down" model that shares all of the core functionality.

The second set of standards could include the remainder of requirements for handicapped access that would be applicable to all systems, regardless of the technology. Any existing systems, in order to maintain their viability, would be required to retrofit. It is not a standard if all systems are not required to meet them. If the Commission believes that the accessibility standards should include voice feedback, then all systems for the handicapped should have voice feedback. But by allowing this proposed separation of systems, not only do the handicapped get what they need, but also the FEC does not put undo burden on the resources of the vendors or on the cash flow of the municipalities. Good for all.

Electrical Provisions

The proposed standards suggest a requirement that mandates a minimum of 16 hours of backup power for all systems, yet exempts lighting from this requirement. We assume if lighting is exempt, so is general power to the facility. If the standard's purpose is to insure that the systems have power so an election is not suspended because of the lack of it, this requirement, as written, is certainly a very expensive and fallible method. There are too many alternatives, such as a standard requiring supplementing conventional uninterruptible power sources with a back-up power generator at each polling center. This would resolve the lighting issue as well and with the popularity of equipment rental companies – could be accomplished in a much less expensive manner. When applying this standard to paper or mechanical based systems, how is a polling center or central counting facility run without lights or power? Either they are standards common for all systems or they are not standards.

CONCLUSION

Accepting Change

Accepting that change is necessary, and thus inevitable, EIP's assertion is that any effective new voting system must successfully integrate the processes of voter registration, voter authentication, vote gathering, and reporting into a secure environment. This must be accomplished through a more rigorous set of voting management standards and approaches. They should be built from the ground up to include at least the current state-of-the-art and provide for the future acceptance of new technology. Failure to consider this paradigm would continue an ineffective development of technology over procedure, which easily leads to micromanagement and immense escalation of costs. A logical extension to this assertion, would acknowledge the necessity for a review and re-engineering of the entire election process.